

UNITED STATES DISTRICT COURT

FILED

for the

JAN 07 2019

Northern District of Oklahoma

Mark C. McCartt, Clerk
U.S. DISTRICT COURT

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)black LG Touchscreen cellular telephone contained in a pink case,
currently located at the DEA, Tulsa Resident Office Evidence Room
held under Case MG-16-0024 as Exhibit N-9.

Case No.

19-mj-6-PJC

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment "A":

located in the Northern District of Oklahoma, there is now concealed (identify the person or describe the property to be seized):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:


Code Section
21 U.S.C. § 846

Offense Description
Conspiracy to possess methamphetamine with the intent to distribute.

The application is based on these facts:

See Affidavit of SA Cory Hallum, DEA, attached hereto.

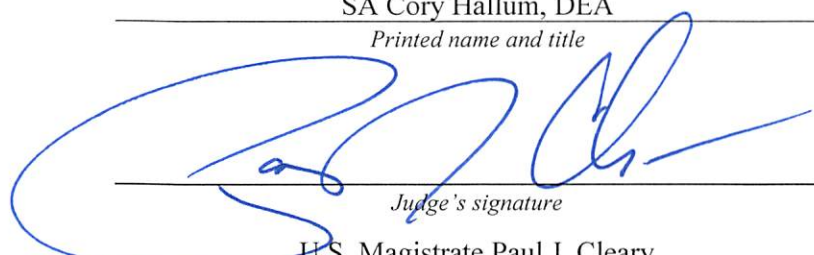
- ☒ Continued on the attached sheet.
☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

SA Cory Hallum, DEA
Printed name and title

Sworn to before me and signed in my presence.

Date: 1/7/2019


Judge's signature

City and state: Tulsa, OK

U.S. Magistrate Paul J. Cleary
Printed name and title

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Cory Hallum, having been duly sworn, do depose and state as follows:

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

INTRODUCTION AND INVESTIGATOR BACKGROUND

2. I am currently employed as a Special Agent with the Drug Enforcement Administration (DEA) and have been so employed since 1998. In February 1999, I was temporarily assigned to the Oklahoma City District Office. In May 1999, I reported to the Houston Field Division, Corpus Christi Resident Office, at which time I was assigned to the High Intensity Drug Trafficking Area (HIDTA) group. I remained an active member of the HIDTA group until 2002 when I was transferred to Enforcement Group One. In June 2006, I was transferred to the Tulsa Resident Office where I am currently assigned to the HIDTA group.

3. This affidavit is intended for the limited purpose of establishing probable cause in support of a search warrant of a cellular telephone belonging to **Karen Pierce**. I believe there will be evidence of the following violation Title 21

United States Code, Section 846, conspiracy to possess methamphetamine with the intent to distribute.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, law enforcement officers, confidential informants (CIs), cooperating witnesses (CWs), and sources of information (SOIs). This affidavit is intended to establish probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is a black LG Touchscreen cellular telephone contained in a pink case, hereinafter the "Device." The Device is currently located at the DEA, Tulsa Resident Office, located at 7615 E. 63rd Place, Suite 250, Tulsa, OK, and held as DEA Exhibit N-9 under investigation MG-16-0024.

6. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. In the fall of 2018, the DEA, Tulsa Resident Office and the FBI, Joplin Office, began investigating an organization that was delivering large amounts of methamphetamine to the Downstream Casino near Joplin, Missouri. The

investigation revealed that Karen Pierce was responsible for transporting the methamphetamine from Oklahoma City, Oklahoma to the Downstream Casino approximately two times each month.

8. On November 14, 2018, investigators received information that Pierce may be traveling from Oklahoma City to Joplin with a load of methamphetamine. The information received indicated that Pierce would be arriving at the Downstream Casino in Joplin at approximately 11:00pm.

9. At approximately 5:00pm, agents established surveillance at Pierce's residence in Oklahoma City. I was contacted Oklahoma Highway Patrol Trooper Cody Hyde and informed him of the situation. I provided trooper HYDE with the description of Pierce and her possible accomplice, Boyett. I also provided Trooper Hyde with a description of Pierce's vehicle (2003 silver Dodge Durango with Oklahoma plates CEW-011).

10. At approximately 7:45pm Trooper Hyde observed the suspected Dodge Durango exit the main traffic lane on I-44 to the toll lane at the Vinita gate and conducted a traffic stop based on independent probable cause.

11. The driver of the vehicle was identified as Karen Pierce and the passenger was identified as Patricia Boyett. Pierce and Boyett indicated to Trooper Hyde that they were traveling to the Downstream Casino in Joplin. A canine, trained in the detection of illegal substances, conducted an open-air, non-intrusive,

search of the exterior of the vehicle. The canine positively alerted to an illegal odor emanating from within the vehicle. Due to the alert of the canine a secondary search of the vehicle was conducted. The search revealed approximately 6 pounds of methamphetamine contained in a red backpack under some women's clothing in the back seat of the Dodge Durango

12. On the same date, investigators with both the DEA and FBI arrived to review the evidence and speak with Pierce and Boyett. Both Pierce and Boyett were advised of the Miranda Warning. Pierce wished to have a lawyer present before any questioning and Boyett agreed to make statements without a lawyer present.

13. Boyett indicated to FBI SA Stacy Moore that she and PIERCE were taking the methamphetamine to the Downstream Casino where they would get a room and sell the methamphetamine. Boyett indicated that Pierce maintained contact with both the source of supply for the methamphetamine and the individuals where the methamphetamine was being delivered.

14. At the time of arrest, Pierce was in possession of one LG cellular telephone contained in a pink case (the Device).

15. The evidence recovered from the vehicle, to include the Device, was turned into the DEA, Tulsa Resident Office, under case MG-16-0024 and labeled as Exhibit N-9.

16. The Device is currently in the lawful possession of the DEA. It came into the DEA's possession in the following way: seized incident to arrest. I seek this warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

17. The Device is currently in evidentiary storage at 7615 E. 63rd Place, Suite 250, Tulsa, OK 74133. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the DEA.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

18. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

19. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that smartphone files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a smartphone, the data

contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, the smartphone may retain a log or record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, electronic storage media may contain electronic evidence of how a device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

20. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Device file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium is a dynamic process. Whether data stored on a device is evidence may depend on other information stored on the computer and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is, or is not, present on a storage medium.

- f. I know that when an individual uses an electronic device as a communication device or a device to obtain information from the Internet related to a criminal act, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

21. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

22. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

23. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.



Cory Hallum, Special Agent
Drug Enforcement Administration

Subscribed and sworn to before me this 3rd day of January 2019:


THE HONORABLE PAUL J. CLEARY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is a black LG Touchscreen cellular telephone contained in a pink case, hereinafter the “Device.” The Device is currently located at the DEA, Tulsa Resident Office Evidence Room held under Case MG-16-0024 as Exhibit N-9.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to being a conspirator in unlawful drug distribution in violation of Title 21, United States Code, Sections 846, including:

- a. records relating to communication with others as to the criminal offenses above; including incoming and outgoing voice messages; text messages; multimedia messages; applications that serve to allow parties to communicate; all call logs; secondary phone number accounts, including those derived from Skype, Line 2, Google Voice, and other applications that can assign roaming phone numbers; and other Internet-based communication media;
- b. records relating to documentation or memorialization of the criminal offenses above, including voice memos, photographs, videos, and other audio and video media, and all ExIF information and metadata attached thereto including device information, geotagging information, and information of the relevant dates related to the media;
- c. records relating to the planning and execution of the criminal offenses above, including Internet activity, including firewall logs, caches, browser history, and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, records of user-typed web addresses, account information, settings, and saved usage information;
- d. application data relating to the criminal offenses above;
- e. lists of customers and related identifying information;
- f. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;

- g. any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);
- f. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. All records and information related the geolocation of the Device at a specific point in time;

4. All records and information related to the coordination, agreement, collaboration, and concerted effort of and with others to violate the statutes listed in Paragraph 1 of this Attachment.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.